数据安全理论与实践

白杨 alicepub@163.com

00 数据安全岗位需求

- 岗位调研情况
- 主要职责分工

4.1 理论知识权重表

项目		初级（%）	中级（%）	高级（%）
基本要求	职业道德	5	5	5
	基础知识	15	10	5
相关知识要求	数据安全管理	30	20	10
	数据安全工程规划设计和实施建设	15	20	15
	数据安全技术开发与运维	15	15	15
	数据安全监测与应急处置	10	15	25
	数据安全评估	10	15	25
合计		100	100	100

数据安全工程技术人员 国家职业标准

4.2 专业能力要求权重表

项目		初级（%）	中级（%）	高级（%）
专业能力要求	数据安全管理	40	25	20
	数据安全工程规划设计和实施建设	15	20	20
	数据安全技术开发与运维	20	20	15
	数据安全监测与应急处置	15	20	20
	数据安全评估	10	15	25
合计		100	100	100

00 课程目标

本课程通过对典型的数据安全技术介绍，并通过理论与实践结合的方式，针对数据全生命周期防护需求，以典型的数据应用场景为例，开展数据安全实践，达到原理指导实践、实践检验原理的学习效果，课程期望达到下面的教学目标：

（1）理解并掌握数据安全基本概念，及数据安全重要性；

（2）了解数据安全生命周期、典型数据安全威胁以及数据安全法律规范；

（3）掌握典型的数据安全技术，包括数据加密、数据脱敏、数据访问控制、数据水印、数据容灾备份、数据安全销毁等；

（4）能够综合运用数据安全技术，夯实学生数据安全实践与应用能力；

（5）通过本学科严谨、丰富的学科文化训练、引导和熏陶学生，完成对勇攀高峰、严谨治学的学生思想认识、思维方式、价值取向的濡染和塑造；通过学习数据安全知识，充分发挥学科文化力量，明确数据安全工作者社会责任，为数据资产安全提供支撑，护航数字经济发展。

00 课程考核要求

- 课时：24+8
- 平时成绩、期末比例：4:6
- 平时成绩：出勤（5%），实验报告（20%），课后作业（5%）、课外实践（5%）
- 实验8学时（数据加密实验、数据脱敏实验、数据访问控制实验、数据水印实验）
- 参考教材：数据安全与治理（清华出版社）、数据安全实践指南（机械工业出版社）、数据安全原理与实践（清华出版社）

00 课程主要内容

- 第一讲 数据安全概述
- 第二讲 数据分类分级
- 第三讲 数据加密
- 第四讲 数据脱敏
- 第五讲 数据访问控制
- 第六讲 数据水印
- 第七讲 数据容灾备份
- 第八讲 数据安全销毁

第1章 数据安全概述

白杨 alicepub@163.com

第1章 数据安全概述

本讲内容概要：

01 第一节—数据基础概述

02 第二节—典型数据处理场景

03 第三节—数据安全概念

04 第四节—数据安全威胁分析

05 第五节—数据安全法律与规范

第1章 数据安全概述

本讲内容概要：

01 第一节—数据基础概述

02 第二节—典型数据处理场景

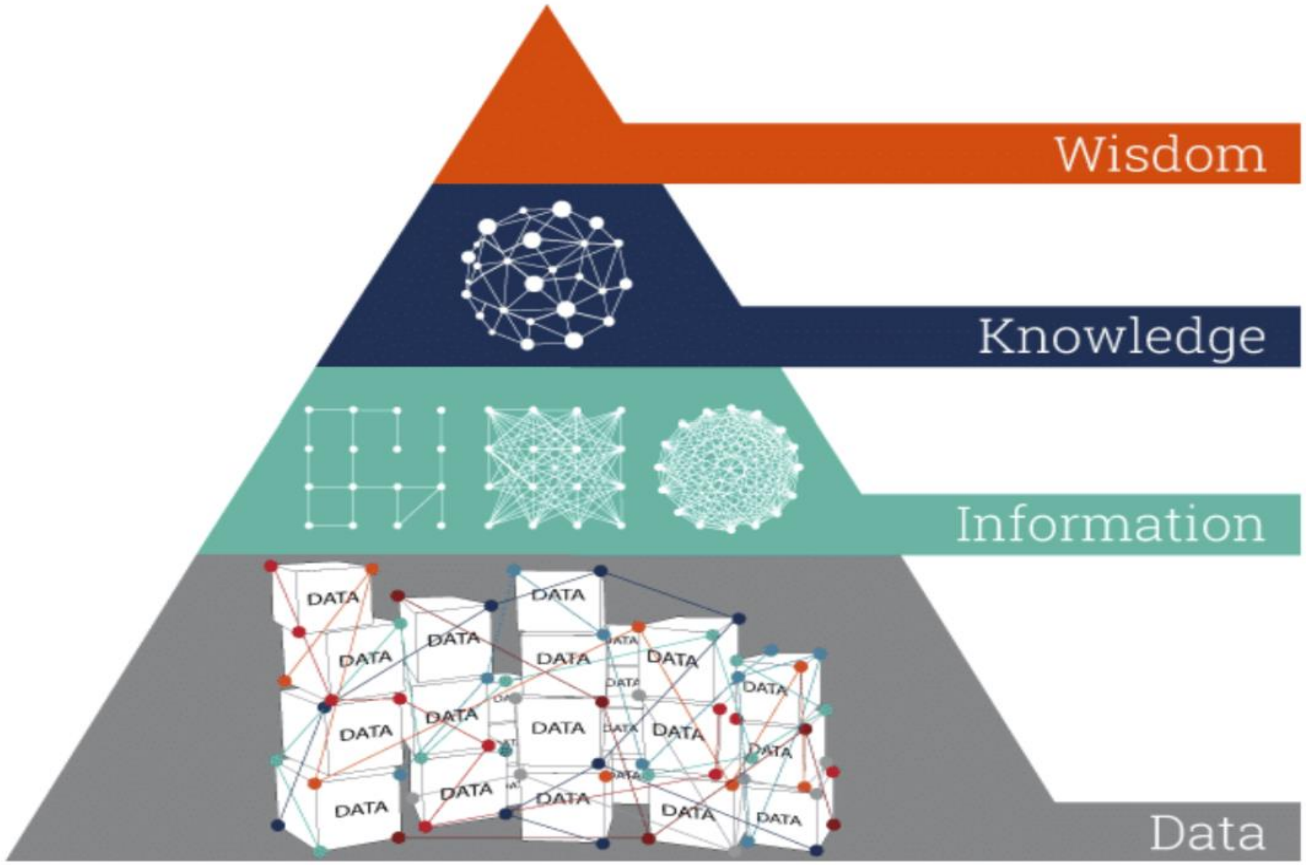
03 第三节—数据安全概念

04 第四节—数据安全威胁分析

05 第五节—数据安全法律与规范

01 1.1 数据基础概述

数据、信息、知识、智慧名词认知



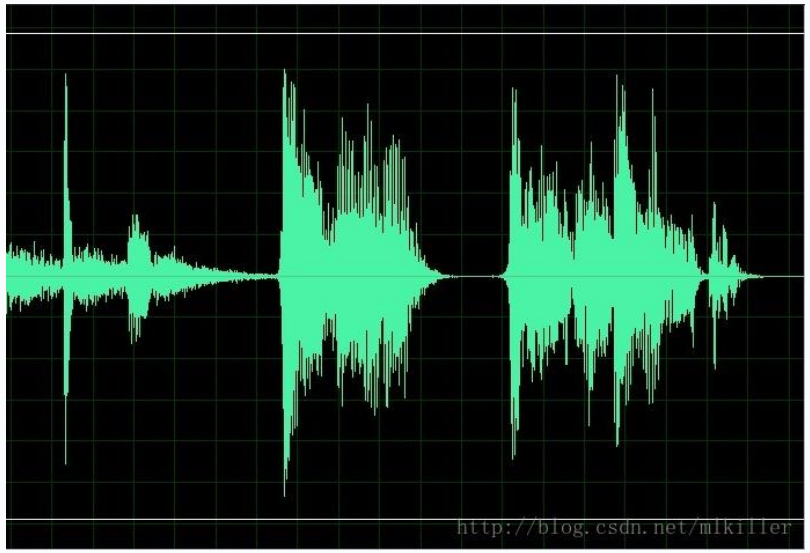
对数据、信息、知识和智慧之间的关系，福特汉姆大学Zeleny教授（1987）提出了**DIKW金字塔模型**（如下图所示），从底层到顶层依次是：

- 数据（Data）：Know nothing，一无所知；
- 信息（Information）：Know what，知道是什么；
- 知识（Knowledge）：Know how，知道怎么做；
- 智慧（Wisdom）：Know why，知道为什么。

01 1.1 数据基础概述

数据的定义：

- 百度百科指出数据是事实或观察的结果，是对客观事物的逻辑归纳，是用于表示客观事物的未经加工的原始素材。数据可以是连续的值，比如声音、图像，称为模拟数据；也可以是离散的，如符号、文字，称为数字数据。在计算机系统中，数据以二进制信息单元0、1的形式表示。
- 数据，按照《中华人民共和国数据安全法》中给出的定义，数据是指任何以电子或者其他方式对信息的记录。由此可见，数据本身可以有丰富的表现形式。



01 1.1 数据基础概述

数据的基本特征：

- 多样性

指数据集中包含不同类型的数据。数据可以是数字、文本、图像、视频等等。这些数据类型都有不同的特征和属性，需要使用不同的方法和技术来处理和分析。

- 分布性

指数据集中数据值的分布情况。数据的分布可以通过绘制直方图、箱线图等图表来可视化。数据的分布可以是正态分布、偏态分布、离散分布等等。

- 关联性

指数据集中不同变量之间的关系。关联性可以通过计算相关系数等统计量来衡量。数据的关联性可以是正相关、负相关或无关。

- 变异性

指数据集中的数据值之间的差异。数据的变异性可以通过测量数据的离散程度来衡量。例如，标准差和方差等统计量可以用来测量数据的变异性。

01 1.1 数据基础概述

大数据的基本特征：

- 数据量大（Volume）
- 类型繁多（Variety）
- 价值密度低（Value）
- 速度快、时效高（Velocity）

01 1.1 数据基础概述

大数据指高速(Velocity) 涌现的大量(Volume) 多样化(Variety) 数据，其特性可简单概括为4V。 简而言之，大数据指非常庞大、复杂的数据集。

大数据的基本特征：

• Volume（海量）

- **数据存储量和计算量大**
- 非结构化数据的超大规模和增长
- 总数据量的80-90%
- 比结构化数据增长快10-50倍
- 是传统数据仓库的10-50倍

• Varity（多样性）

- **要处理的数据来源多、格式多**
- 很多不同形式的数据（文本、图像、视频、机器数据））
- 无模式或者模式不明显
- 不连贯的语法或句义
- 需要进行清洗，整理，筛选等操作

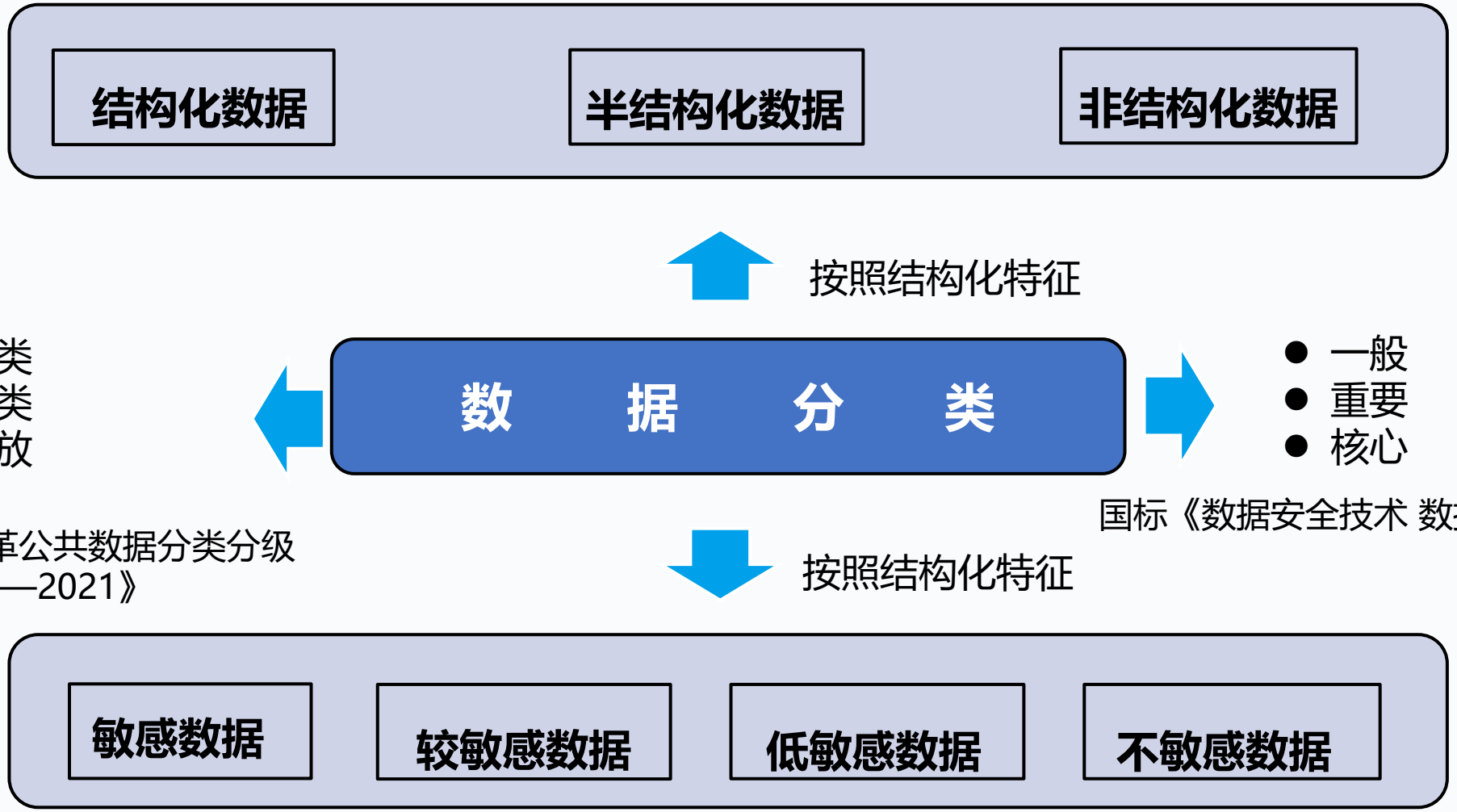
• Velocity（高速）

- **数据增长速度和处理速度快**
- **实时分析**而非批量式分析
- 数据输入、处理与丢弃
- 立竿见影而非事后见效

• Value（价值）

- **数据价值密度低的特点**
- 大量不相关信息
- 对外来趋势与模式的可预测分析
- 深度复杂分析（机器学习、人工智能VS传统商务智能（咨询、报告等））

01 1.1 数据基础概述



浙江省《数字化改革 公共数据分类分级指南 DB33/T 2351—2021》
四川省《政务数据 数据分类分级指南 DB51/T 3056—2023》

01 1.1 数据基础概述

1. 结构化特征标准分类

1) 结构化数据

结构化数据也称为定量数据，指符合预定义结构或模型的数据。具有明确定义的数据格式和组织方式，通常以表格、数据库记录等形式存储，易于通过计算机程序进行处理和分析。主要使用关系型数据库表示和存储，可以用二维表来逻辑表达实现。比如：Excel、mysql（参见图1. 1）、企业ERP、OA、HR里的数据。

id	name	age	gender
1	Liu Yi	20	male
2	Chen Er	35	female
3	Zhang San	28	male

图1. 1 结构化数据—Excel

01 1.1 数据基础概述

1. 结构化特征标准分类

2)半结构化数据

半结构化数据并不符合关系型数据库或其他数据表的形式关联起来的数据模型结构，但包含相关标记，用来分隔语义元素以及对记录和字段进行分层，数据的结构和内容混在一起，没有明显的区分，因此，它也被称为自描述的结构，简单的说半结构化数据就是介于完全结构化数据和完全无结构的数据之间的数据。最为常见的半结构化数据包括日志文件、XML 文档、JSON 文档、Email、HTML文档（参见图1. 2）等。

```
<person>
    <name>A</name>
    <age>13</age>
    <gender>female</gender>
</person>


<person>
    <name>B</name>
    <gender>male</gender>
</person>
```

图1. 2 半结构化数据—HTML文档

01 1.1 数据基础概述

1. 结构化特征标准分类

3)非结构化数据

非结构化数据是定性数据，没有内部结构，没有固定的数据模型或组织形式，通常保存为不同类型的文件，例如文本文件、图片、音频、视频等（参见图1. 3），通常需要特殊的技术和工具才能进行有效处理和分析。

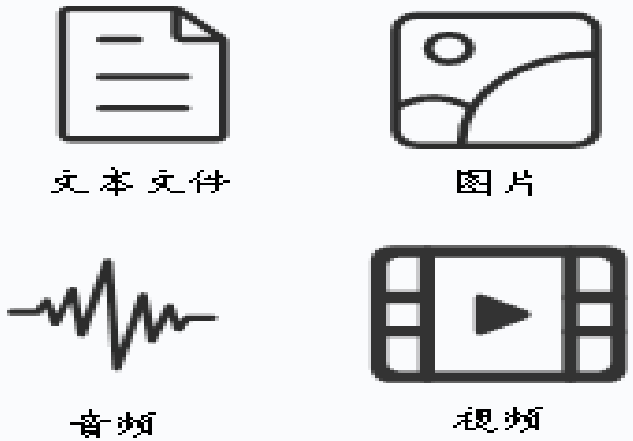


图1. 3 非结构化数据

01 1.1 数据基础概述

2. 敏感性级别标准分类

根据四川省《政务数据 数据分类分级指南 DB51/T 3056—2023》[5]，数据的安全级别可按照数据的安全属性破坏后的影响对象、影响程度划分为四级，由高至低分别为：极敏感级(四级)、敏感级(三级)、低敏感数据(二级)、不敏感数据(一级)。

1)极敏感级(四级)

数据遭到破坏后，对国家安全轻微影响、中等影响或者严重影响，对社会秩序及公共利益造成中等影响或者严重影响，对政府机构、企事业单位及其他社会组织造成严重影响，个人权益造成严重影响。数据特性如下：

- 数据一般不可被共享和开放，或可通过申请向特定单位或人员公开。
- 数据发生泄露、篡改、丢失或滥用后，对个人权益、政府机构、企事业单位及其他社会组织造成严重影响；对社会秩序及公共利益造成中等及以上影响；对国家安全造成影响。

01 1.1 数据基础概述

2. 敏感性级别标准分类

根据四川省《政务数据 数据分类分级指南 DB51/T 3056—2023》[5]，数据的安全级别可按照数据的安全属性破坏后的影响对象、影响程度划分为四级，由高至低分别为：极敏感级(四级)、敏感级(三级)、低敏感数据(二级)、不敏感数据(一级)。

2)敏感级(三级)

数据遭到破坏后，对国家安全无影响，对社会秩序及公共利益造成轻微影响，对政府机构、企事业单位及其他社会组织造成中等影响，对个人权益造成中等影响。数据特性如下：

- 数据可进行有条件共享和开放。可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用；可提供给部分或部分提供给个人和组织开放使用。
- 数据发生泄露、篡改、丢失或滥用后，对个人权益、政府机构、企事业单位及其他社会组织的正常运作和合法权益造成中等影响；对社会秩序及公共利益造成轻微影响；对国家安全不造成影响。

01 1.1 数据基础概述

2. 敏感性级别标准分类

根据四川省《政务数据 数据分类分级指南 DB51/T 3056—2023》[5]，数据的安全级别可按照数据的安全属性破坏后的影响对象、影响程度划分为四级，由高至低分别为：极敏感级(四级)、敏感级(三级)、低敏感数据(二级)、不敏感数据(一级)。

3)低敏感级(二级)

数据遭到破坏后，对国家安全无影响，对社会秩序及公共利益无影响，对政府机构、企事业单位及其他社会组织造成轻微影响，对个人权益造成中等影响。数据特性如下：

- 数据可进行有条件共享和开放。可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用；可提供给部分或部分提供给个人和组织使用。
- 数据发生泄露、篡改、丢失或滥用后，对个人权益、政府机构、企事业单位及其他社会组织的正常运作及合法权益造成轻微影响；对社会秩序及公共利益、国家安全不造成影响。

01 1.1 数据基础概述

2. 敏感性级别标准分类

根据四川省《政务数据 数据分类分级指南 DB51/T 3056—2023》[5]，数据的安全级别可按照数据的安全属性破坏后的影响对象、影响程度划分为四级，由高至低分别为：极敏感级(四级)、敏感级(三级)、低敏感数据(二级)、不敏感数据(一级)。

4)非敏感(一级)

数据遭到破坏后，对国家安全、社会秩序及公共利益无影响、政府机构、企事业单位及其他社会组织、个人权益无影响。数据特性如下：

- 原则可提供给所有政务部门共享使用并面向社会完全开放或脱敏后开放。
- 数据发生泄露、篡改、丢失或滥用后，对个人权益、政府机构、企事业单位及其他社会组织的正常运作及合法权益不造成影响或影响微弱可以忽略；对社会秩序、公共利益以及国家安全不造成影响。

01 1.1 数据基础概述

3．3．安全保护标准分类

根据四川省《政务数据 数据分类分级指南 DB51/T 3056—2023》，政务数据按照开放属性可分为：不予开放/有条件开放类、有条件开放类、无条件开放类。

1)不予开放/有条件开放类

不宜提供给任何自然人、法人和非法人组织开放使用，原则上不予开放，或在不违反法律法规的条件下提供可用不可见的有条件开放。

2)有条件开放类

可提供给部分自然人、法人和非法人组织使用，仅能够部分提供给所有自然人、法人和非法人组织开放使用或在不违反法律法规的条件下，面向社会脱敏后有条件开放。

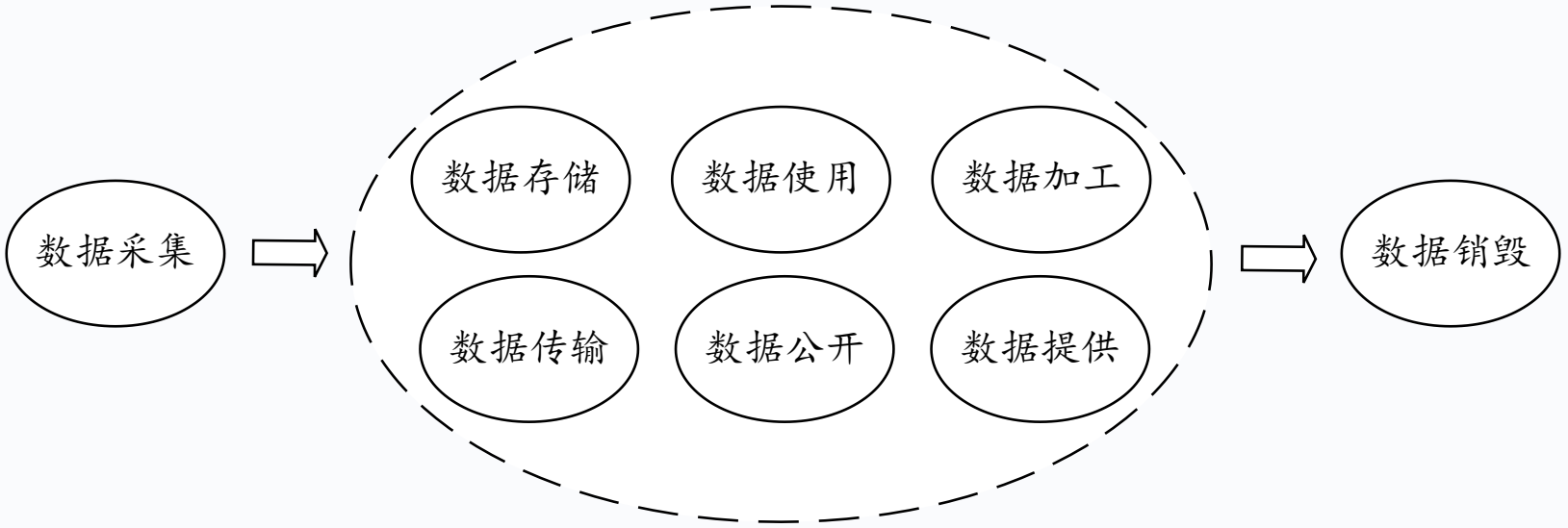
3)无条件开放类

原则上在不违反法律法规的条件下，面向社会完全开放或脱敏后开放。

01 1.1 数据基础概述

数据生命周期：

国家标准《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》中给出了数据生存周期的6个阶段，它是从数据处理的各个阶段来划分的，本质上是一种派生数据处理过程。而《中华人民共和国数据安全法》中指出：“数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等”。因此，数据生命周期，共包含8个阶段，这里将它称为动态数据生命周期，其各个阶段分别是：“数据采集、数据存储、数据使用、数据加工、数据传输、数据提供、数据公开和数据销毁”。特定的数据所经历的生存周期由实际的业务所决定，可为完整的8个阶段或是其中的几个阶段。



01 1.1 数据基础概述

数据生命周期：

数据采集	数据存储	数据使用	数据加工
指从外部收集数据和在企业内部系统中生成新数据的阶段。	指将数据保存在持久性存储介质中，以便后续访问、处理和保留，通常用于长期保存数据。	指利用存储在各种数据存储介质中的数据来进行分析、处理、应用和决策的过程。	指在数据生命周期中对数据进行各种操作，包括清洗、转换、整合、分析和应用。

01 1.1 数据基础概述

数据生命周期：

数据传输	数据提供	数据公开	数据销毁
指数据从一个实体传送到另一个实体的阶段，旨在实现数据共享、通信或备份等目的。	指为个人，企业或组织提供数据的过程。数据提供者可以是个人、组织或系统	指将数据向公众开放和可访问，以促进数据的共享、透明度和创新。	指数据承载的模块、设备、系统在弃置、转售、捐赠前或因数据不在需要彻底清除所存储的数据。

第1章 数据安全概述

本讲内容概要：

01 第一节—数据基础概述

02 第二节—典型数据处理场景

03 第三节—数据安全概念

04 第四节—数据安全威胁分析

05 第五节—数据安全法律与规范

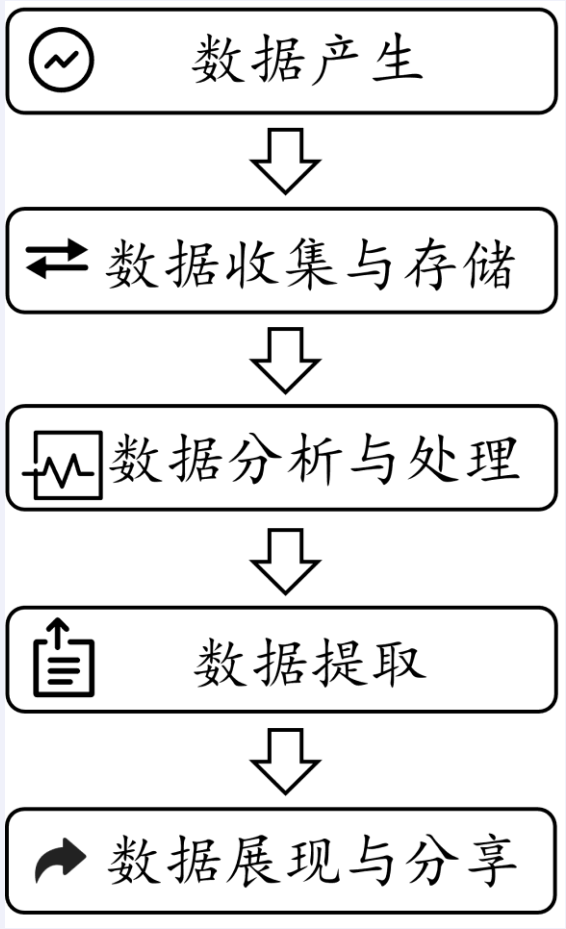
02 1.2 典型数据处理场景

典型数据处理场景包括以下场景：

- 数据开发利用场景
- 数据合作共享场景
- 数据交易场景
- 大数据处理场景
- 多方数据融合场景
- 数据跨境场景

02 1.2 典型数据处理场景

数据开发利用场景



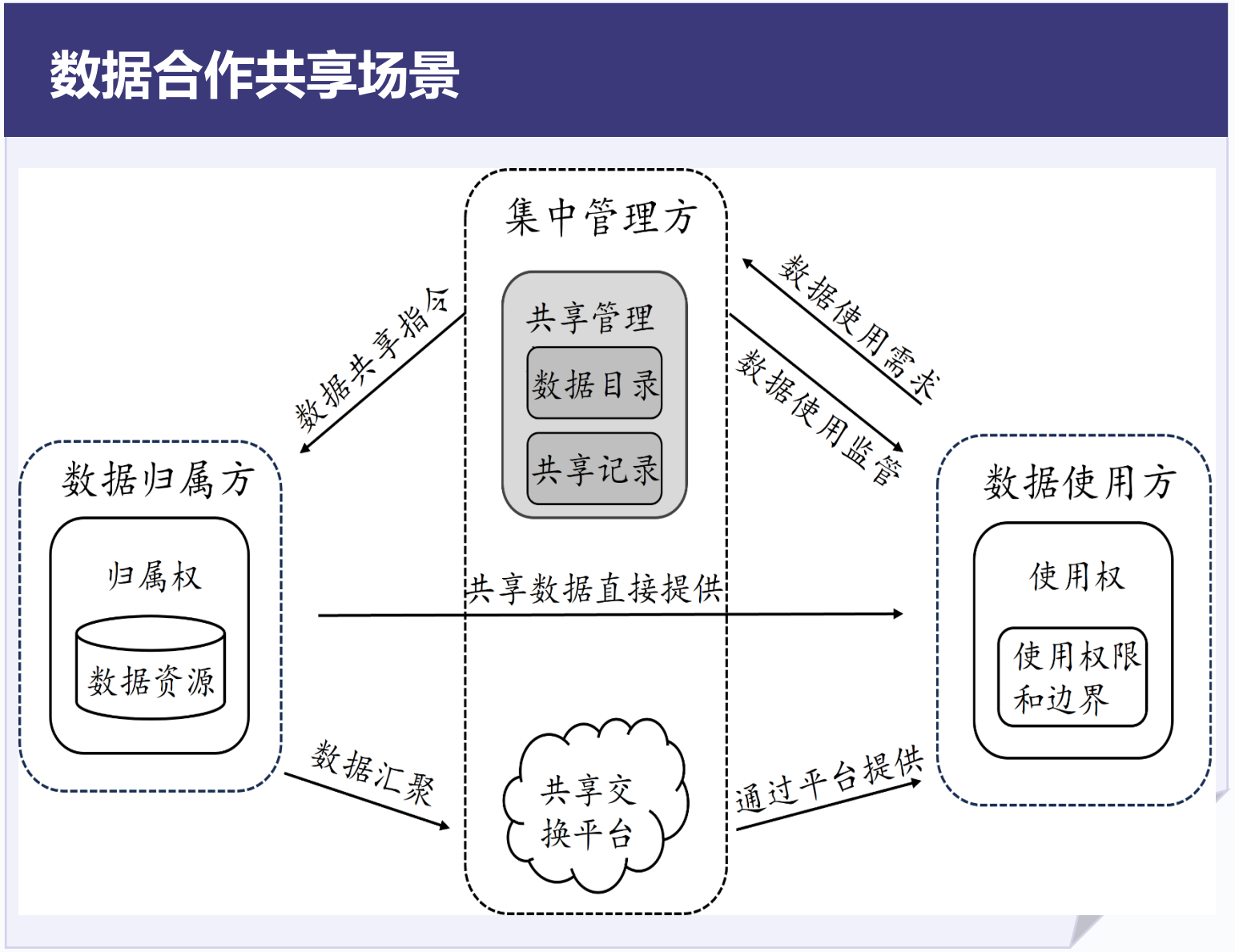
数据开发利用场景

数据开发利用场景通过各种系统和设备产生海量数据，然后将这些数据收集与存储起来，进行数据分析与处理，从中提取有价值的信息，并通过数据展现与分享的方式传达给相关人员，帮助他们做出更明智的决策。其主要目的是提供有价值的数据支持和洞察。数据开发在各个行业和领域都有广泛的应用场景，如零售和电商行业、金融服务行业、医疗保健行业，制造业……

02 1.2 典型数据处理场景

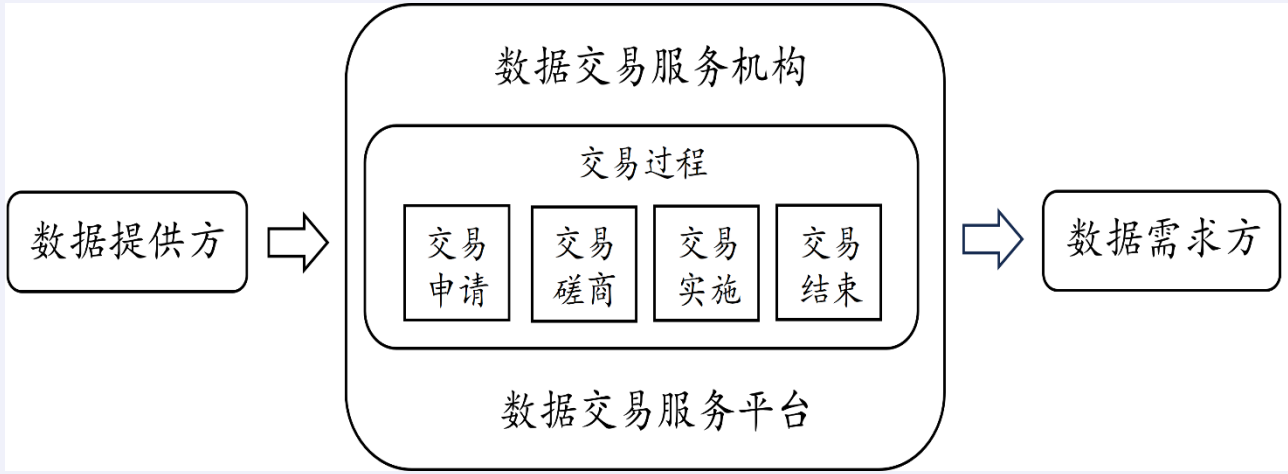
数据合作共享场景

数据合作共享场景主要有三种方式。第一种，**参与对象主要包括数据归属方、数据使用方和集中管理方**，数据归属方拥有数据资源的归属权，数据使用方拥有数据使用权（包含使用权限和边界），集中管理方拥有共享管理权（主要负责数据目录和共享记录）。数据使用方可以向集中管理方提出使用需求，然后集中管理方给数据归属方发送数据共享指令。数据集中管理方对数据使用方具有数据使用监管的责任。第二种，**数据归属方直接给数据使用方提供共享数据**。最后一种方式则是**通过共享交换平台进行合作共享，数据使用方将数据汇集到共享交换平台，通过平台提供数据资源给数据使用方**。



02 1.2 典型数据处理场景

数据交易场景



数据交易场景

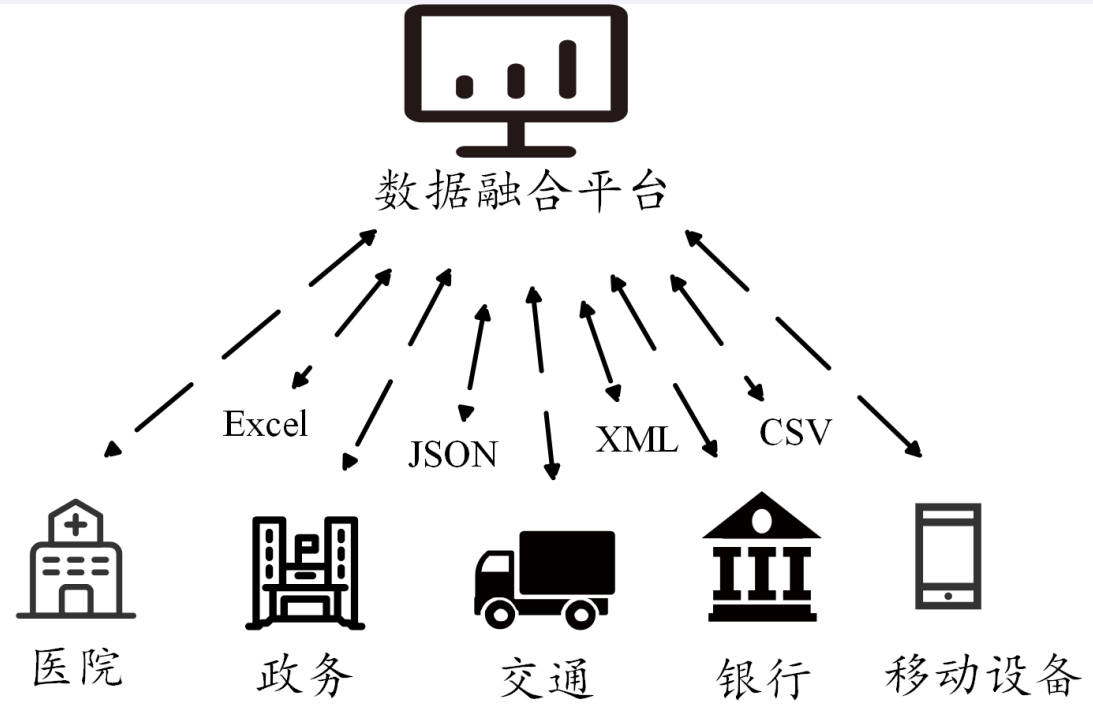
数据交易场景参与对象主要包括**数据提供方、数据需求方和数据交易服务机构**（数据交易服务平台）。数据交易法务机构主要负责交易过程，即包括交易申请，交易磋商，交易实施，交易结束。

02 1.2 典型数据处理场景

多方数据融合场景

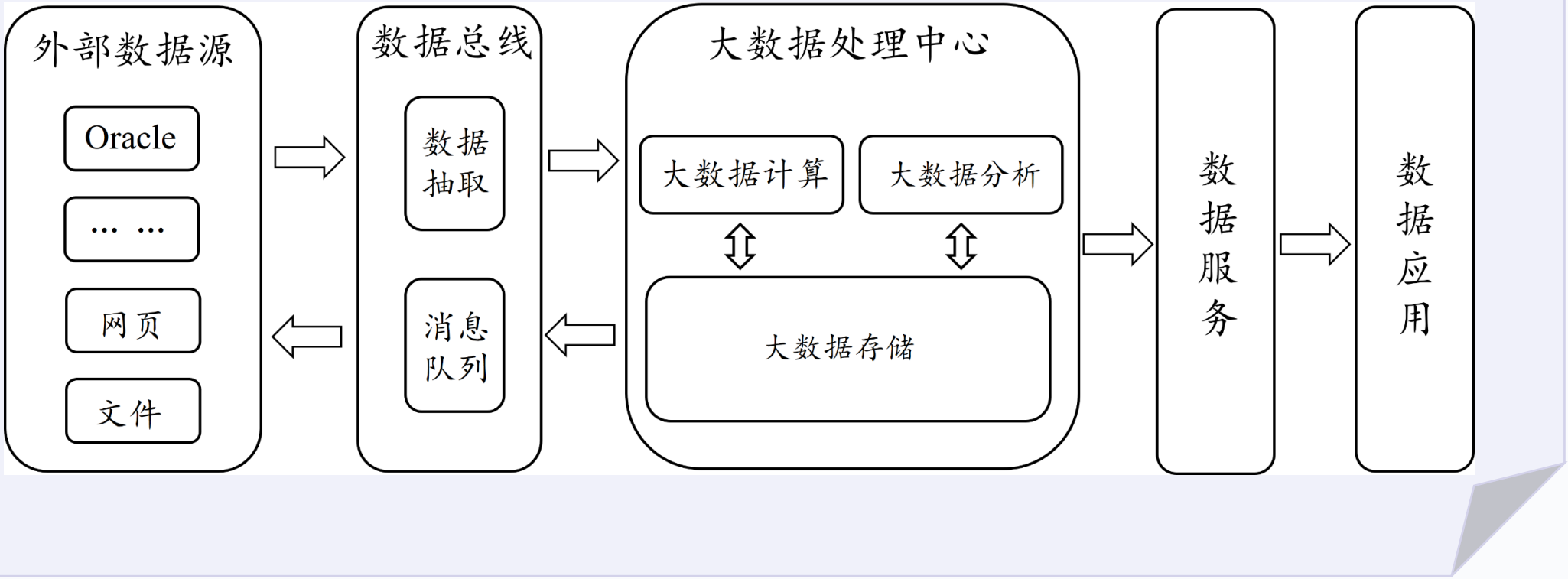
多方数据融合场景指的是整合来自不同来源、不同格式、不同领域的数据，进行综合分析和挖掘的过程。在这种场景下，各方可以共享、整合和利用各自的数据资源，实现跨部门、跨组织的数据共享与应用，从而产生更全面、更深入的见解和价值。通过多方数据融合，可以实现数据的互通互联，促进信息共享和智能决策，推动创新发展和智慧应用。

多方数据融合场景



02 1.2 典型数据处理场景

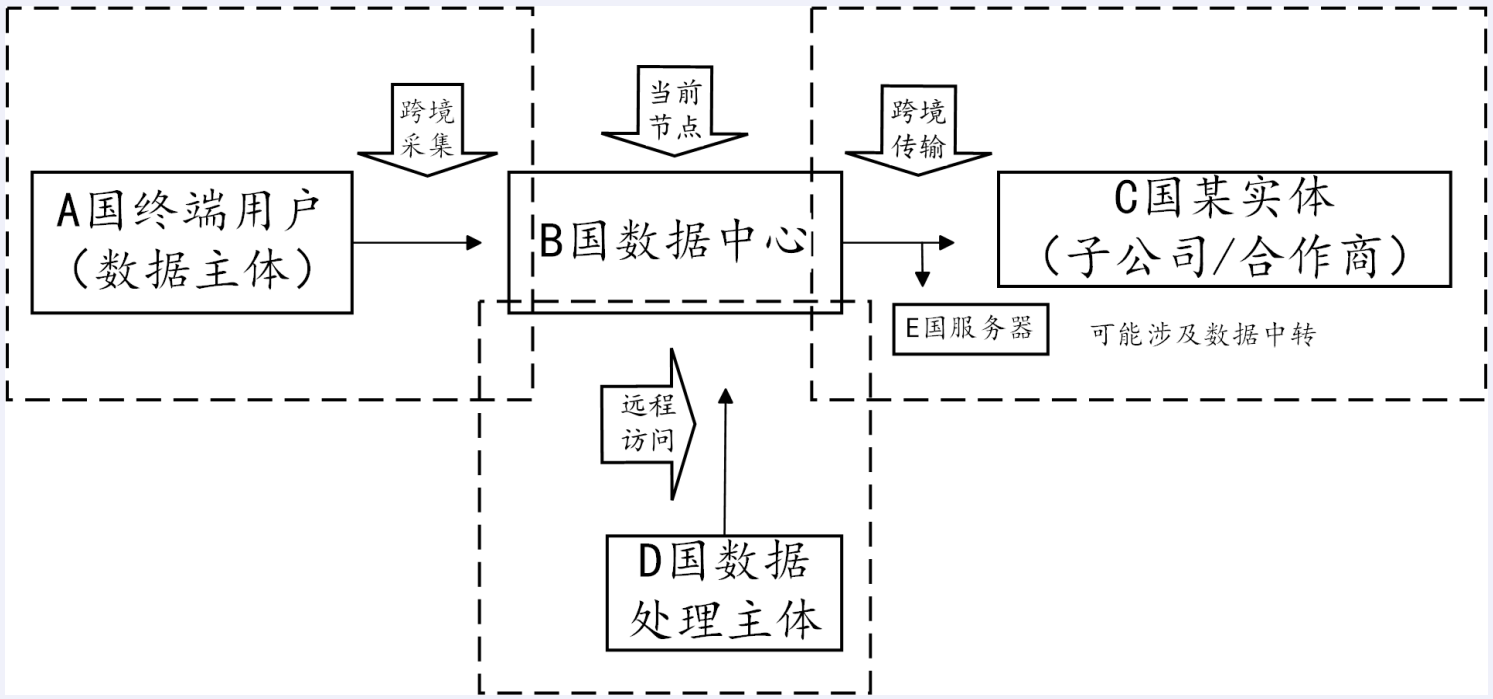
大数据处理场景



大数据处理场景参与对象主要包括外部数据源（大数据提供者），数据总线（负责数据抽取和消息队列），大数据处理中心（负责大数据计算、大数据分析和大数据存储），数据服务者，数据应用提供者。数据总线对外部数据源的数据进行数据抽取，再将数据提交给大数据处理中心，数据在此可进行计算和分析。

02 1.2 典型数据处理场景

数据跨境场景



数据跨境场景指的是数据在不同国家或地区之间的流动和应用。在这种场景下，数据可以以跨境贸易、国际合作、全球化业务等形式进行传输和交换。**数据跨境涉及到数据的安全、隐私保护、法律合规等复杂问题，需要考虑不同国家或地区的数据保护法规和政策要求**。同时，数据跨境也带来了巨大的机遇，可以促进跨国企业合作、推动创新发展、支持全球化经济。在数据跨境场景中，重要的是平衡数据的自由流动与数据安全保护之间的关系，确保数据的合法合规和双方利益的平衡

第1章 数据安全概述

本讲内容概要：

01 第一节—数据基础概述

02 第二节—典型数据处理场景

03 第三节—数据安全概念

04 第四节—数据安全威胁分析

05 第五节—数据安全法律与规范

03 1.3 数据安全概念

01

数据安全是组织保护其数字信息免遭未经授权的访问、使用、修改、损坏、利用、丢失和盗窃的流程。

03

数据安全有助于在其整个生命周期中保护敏感数据，了解用户活动和数据的上下文，并防止未经授权使用数据或丢失数据。

05

《数据安全法》

Elastic公司

Oracle公司

微软公司

华为云

指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

02

数据安全性是指采用保护措施来防止数据受到未经批准的访问并保持数据机密性、完整性和可用性。

04

数据安全有对立的两方面的含义：一是数据本身的安全，主要是指采用现代密码算法对数据进行主动保护。二是数据防护的安全，主要是采用现代信息存储手段对数据进行主动防护。

03 1.3 数据安全概念

◆ 机密性

数据安全首先要求数据在存储、传输和处理过程中不被未经授权的人员或系统访问和使用。

◆ 完整性

指确保数据的准确性和完整性，防止数据在传输或存储过程中被篡改或损坏。

◆ 可用性

指确保数据在需要时可随时使用和访问。数据应该在合理的时间范围内可供授权用户使用，不受任何不可预见的干扰或故障的影响。

数据安全内涵与三要素

数据安全的内涵指的是保护数据的机密性、完整性和可用性，建立有效的访问控制和权限管理机制，遵守法律法规和行业标准，采取防护措施预防恶意攻击，以及进行数据安全风险管理，从而确保数据在存储、传输和处理过程中的安全性和隐私性。其中，数据的机密性、完整性和可用性是数据安全的三要素。

第1章 数据安全概述

本讲内容概要：

01 第一节—数据基础概述

02 第二节—典型数据处理场景

03 第三节—数据安全概念

04 第四节—数据安全威胁分析

05 第五节—数据安全法律与规范

04 1.4 数据安全威胁分析

黑客攻击

指黑客通过各种手段（如SQL注入、跨站脚本攻击、钓鱼邮件等）获取系统或网络中的敏感信息，包括用户名、密码、信用卡号、企业机密等。

MOVEit Transfer数据盗窃攻击利用了MOVEit文件传输工具中的漏洞，攻击者未使用加密机制，而是以非法泄露数据作为勒索条件。

防护手段：在现实的网络环境中，要防范黑客攻击的措施主要是从两方面入手：建立具有安全防护能力的网络和改善已有网络环境的安全状况；强化网络专业管理人员和计算机用户的安全防范意识，提高防止黑客攻击的技术水平和应急处理能力。

2023年5月，勒索软件Clop组织利用Progress的MOVEit文件传输工具中的一个严重漏洞，开始了大规模的勒索软件攻击活动。与传统的勒索软件攻击不同，本次的攻击行动并没有采用任何加密机制，而是以非法泄露数据作为勒索条件。Clop声称，如果受害者公司支付赎金，它将不会在其暗网网站上泄露受害者的被盗数据。针对数百家选择不支付赎金的公司，Clop确实是这么做的。

目前尚不清楚哪些公司实际上支付了赎金。但据网络安全事件响应公司Coveware估计，Clop将从攻击活动中获利7500万美元至1亿美元。截至目前，受MOVEit活动影响的组织总数或许已经接近3000家。就已知受影响的个人而言，如今总数接近8400万人。这使其成为2023年影响最广泛的攻击之一，也使其成为近年来最严重的数据泄露事件之一。在IT行业，MOVEit数据勒索活动的受害者包括IBM、高知特、德勤、普华永道和安永。

04 1.4 数据安全威胁分析

恶意软件

恶意软件（如勒索软件、木马、蠕虫等）能潜入系统，破坏数据、篡改文件、传播自身，甚至发起分布式拒绝服务攻击。

在ESXi勒索软件攻击事件中，攻击者利用一个已知漏洞来入侵运行VMware ESXi虚拟机管理程序的服务器。该漏洞可以远程执行代码，使攻击者能够获取对服务器的控制权。攻击者通过安装勒索软件对受影响的服务器进行加密，并要求受害者支付赎金以解密其数据。

防护手段：采用反病毒软件和恶意软件防御工具，设置实时扫描和自动隔离功能；部署安全事件管理系统，以便快速响应和处理疑似感染事件；定期对设备进行漏洞扫描，修补已知的安全漏洞。

2023年2月，“ESXiArgs”勒索软件组织攻击了运行VMware ESXi虚拟机管理程序的客户。据美国联邦调查局和美国计算机安全管理局调查数据显示，全球受到攻击影响的服务器数量超过了3800台。

据网络安全供应商Censys的安全研究人员介绍，这起活动的目标主要是针对美国、加拿大、法国和德国等国家的企业组织，攻击者利用了一个已经存在两年之久的漏洞（编号为CVE-2021-21974），主要影响旧版本VMware ESXi中的OpenSLP服务，可以被用来远程执行代码。此次ESXiArgs勒索软件攻击事件，再次凸显了保护虚拟化应用基础设施的重要性。

在提交给蒙大拿州总检察长办公室的安全事件通知中，该公司解释说，攻击行为发生在2022年12月23日，但直到27天后的2023年1月10日，百事可乐才检测到攻击，修复则需要更长的时间。

04 1.4 数据安全威胁分析

社交工程攻击

指利用人性弱点，如信任感缺失、好奇心驱使等，诱骗用户透露个人信息或执行危险操作（如钓鱼邮件，冒充身份，社交工程电话）。

攻击者可能发送伪装成正规求助或紧急通知的电子邮件给赌场运营商的IT求助台，要求他们采取某种行动，如点击恶意链接、下载附件或提供敏感信息。

防护手段：应培养公众增强信息安全意识，提高防范“钓鱼”电话、冒充官方机构诈骗邮件、虚假网站登录等社交工程手段的能力。同时，采取必要的安全措施和技术手段，如防火墙、入侵检测系统、数据加密等，保护企业信息和资产的安全；建立健全内部沟通流程和紧急联络渠道。

2023年9月份，攻击者针对赌场运营商米高梅和凯撒娱乐发起了极具破坏性的攻击，攻击手法包括利用社会工程伎俩欺骗IT求助台，非法进入米高梅的网络系统。在此次攻击的调查中还发现，一个名为Scattered Spider的年轻黑客组织与俄罗斯背景的勒索软件团伙Alphv相互勾结、狼狈为奸。

据安全研究人员声称，Scattered Spider的黑客使用了Alphv提供的BlackCat勒索软件（Alphv团伙的成员之前隶属于发动Colonial Pipeline攻击的DarkSide团伙）。虽然多年来勒索软件即服务在东欧一直日益猖獗，但欧美黑客与俄罗斯背景黑客团伙结为联盟似乎再让威胁领域向更加令人不安的新方向发展。

04 1.4 数据安全威胁分析

物联网安全问题

物联网安全问题指的是与物联网设备、网络和数据相关的安全隐患和挑战。

在受影响的设备中，包括了支持物联网的Catalyst 9800无线控制器和Catalyst 9100 接入点。这些设备通常用于连接和管理物联网设备，例如智能家居设备、工业传感器、智能城市设备等。因此，漏洞的利用可能会导致对物联网设备的远程控制、信息窃取或其他恶意操作。

防护手段：第一，采用安全设计原则，为设备固件和通信协议增加认证、加密、身份验证等功能；第二，加强对物联网设备供应商的筛选与评估，确保其具备良好的安全管理体系和合规性；第三，对联网设备进行安全配置管理和定期升级维护，防止潜在风险。

2023年10月中旬，针对思科 IOS XE 客户的攻击迅速成为有史以来影响最广泛的边缘攻击之一。据Censys 研究人员表示，10月16日发现的一个严重 IOS XE 漏洞导致近42000 台思科设备中招。这些产品包括分支路由器、工业路由器和聚合路由器，以及Catalyst 9100 接入点和支持物联网的Catalyst 9800无线控制器。

第1章 数据安全概述

本讲内容概要：

01 第一节—数据基础概述

02 第二节—典型数据处理场景

03 第三节—数据安全概念

04 第四节—数据安全威胁分析

05 第五节—数据安全法律与规范

05 1.5 数据安全法律与规范

《中华人民共和国网络安全法》

《中华人民共和国网络安全法》（简称《网络安全法》）从法律层面保障了广大人民群众在网络空间的利益，有效维护了国家网络空间主权和安全，是国家基本法律。该法于2016年11月通过，于2017年6月施行，是中国首部针对网络安全领域的法律，规定了网络安全的基本要求、责任和义务，以及网络安全管理、网络安全技术、网络安全应急处置等方面的内容。

《网络安全法》第21条构建了网络安全等级保护制度，国家根据信息系统的重要性和对国家安全、经济社会运行的影响程度，将信息系统划分为不同的网络安全等级，实施相应的安全保护措施。

05 1.5 数据安全法律与规范

《中华人民共和国数据安全法》

《中华人民共和国数据安全法》（以下简称《数据安全法》）是数据安全领域的基础性法律，该法于2021年6月通过，于2021年9月施行，是中国首部专门针对数据安全领域的法律，规定了数据安全的基本要求、责任和义务，以及数据安全管理、数据安全保护、数据安全监测预警等方面的内容，对数据开发利用与数据安全并重。

《数据安全法》第21条确立了以数据分类分级为核心的安全制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。

05 1.5 数据安全法律与规范

《中华人民共和国个人信息保护法》

《中华人民共和国个人信息保护法》于2021年8月20日通过，自2021年11月1日起施行，且与《数据安全法》一起从法律层面提供了数据安全保障和个人信息保护。这部法律以数据中的“个人信息”为主要规范对象，划定个人信息全生命周期处理的安全保护规则，以保护个人信息权益、促进个人信息合理利用。

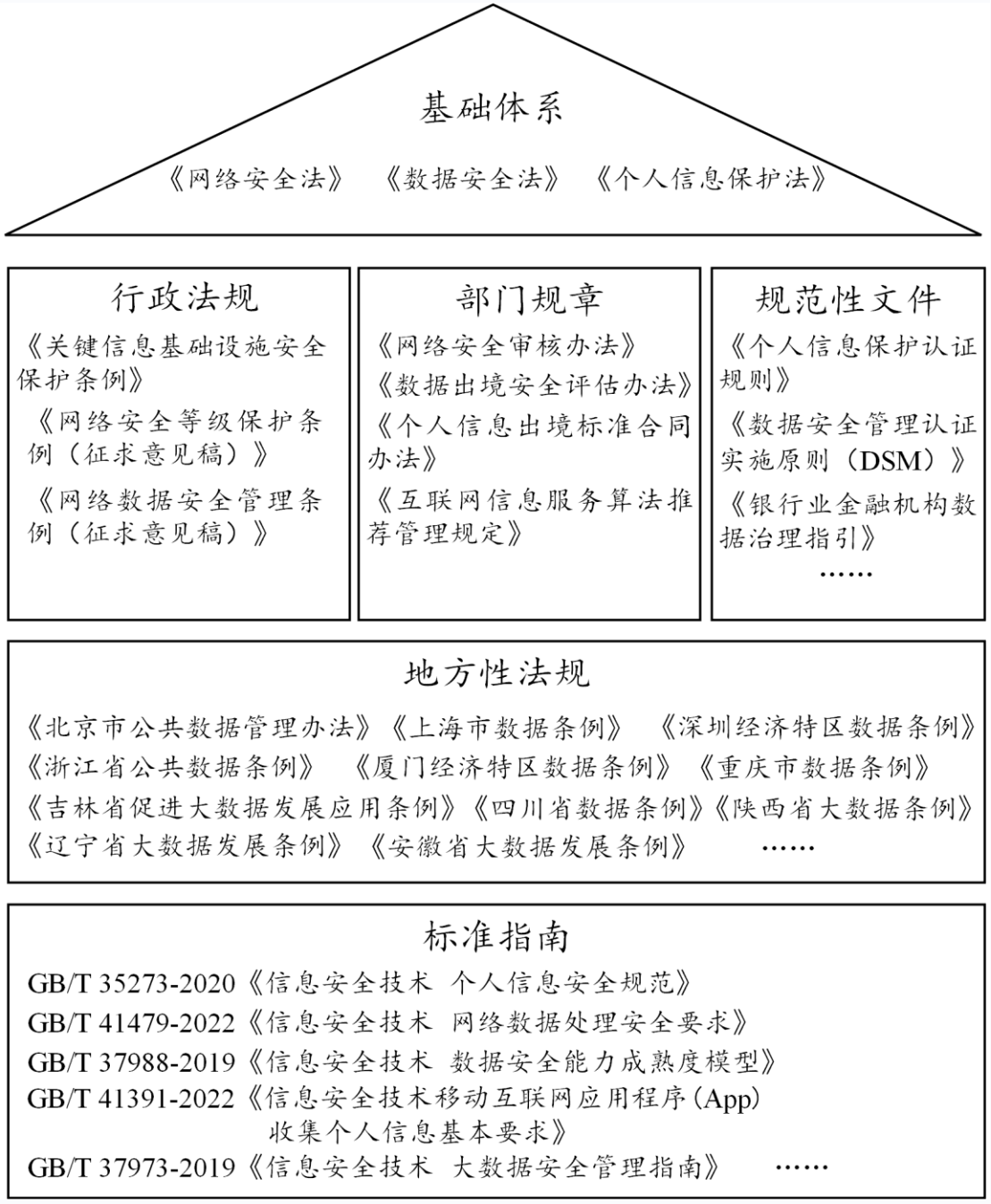
根据《个人信息保护法》，个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等的全生命周期，相应个人信息处理的风险也贯穿于个人信息处理的始终。

05 1.5 数据安全法律与规范

整体法律脉络

- 《中华人民共和国网络安全法》
- 《中华人民共和国数据安全法》
- 《中华人民共和国个人信息保护法》

共同构成了我国数据保护的基础体系，整体的法律法规脉络关系如右图：



05 1.5 数据安全法律与规范

《欧盟网络与信息安全指令》（NIS）

该指令于2016年7月6日颁布，是欧盟针对网络和信息安全问题制定的法规，要求成员国采取措施加强关键网络基础设施的安全保护。该指令明确了关键基础设施的定义和范围，要求成员国对这些设施进行识别和保护，并采取必要的技术和管理措施来防范网络攻击和数据泄露。

欧盟《通用数据保护条例》（GDPR）

该条例于2018年5月生效，是欧盟首部专门针对个人数据保护的法律，规定了个人数据处理的基本要求、责任和义务，以及个人数据保护、隐私保护等方面的内容。GDPR 面向所有收集、处理、储存、管理欧盟公民个人数据的企业，限制了收集与处理用户个人信息的权限，将个人信息的最终控制权交还给用户本人，凡涉及欧盟个人数据的行为，都可被 GDPR 所管辖。在个人数据保护方面，GDPR 是目前全球规定最为严格、处罚最为严厉的法规之一。

05 1.5 数据安全法律与规范

《非个人数据自由流动条例》

2018/1807号条例《非个人数据自由流动条例》于2018年11月14日发布，该条例对数据本地化要求、主管当局的数据获取及跨境合作、专业用户的数据迁移等问题作出了具体规定，并考虑了服务提供商负担过度及市场扭曲等问题，进一步完善了欧盟数据治理框架。

《2019网络安全法案》

2019年4月17日，第2019/881号条例《关于ENISA和信息通信技术网络安全认证的条例》(又称《2019网络安全法案》)正式颁布，这是欧盟网络安全治理的里程碑事件。法案指定欧盟网络和信息安全署(ENISA)为永久性欧盟网络安全机构，确立了第一份欧盟范围的网络安全认证计划，以确保向欧盟境内提供的产品、服务满足其网络安全标准。

05 1.5 数据安全法律与规范

美国《加州消费者隐私法案》（CCPA）

该法案于2018年通过，于2020年生效，是加州首部专门针对消费者隐私保护的法律，规定了消费者个人数据处理的基本要求、责任和义务，以及消费者隐私保护、数据泄露通知等方面的内容。

《联邦数据战略与2020年行动计划》

美国发布《联邦数据战略与2020年行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全性等基本原则。二是强化数据及个人信息保护方面的相关立法。

《个人数据保护法(修订)》草案

2020年5月14日，新加坡通信信息部和个人数据保护委员会联合发布《个人数据保护法(修订)》草案，是规范个人数据收集、使用和披露的综合性立法。为配合该法更好执行，当地还配套出台了特定领域(如电信、房地产、教育、医疗、社会公益服务等行业)的个人数据保护指南。

05 1.5 数据安全法律与规范

数据安全处罚案例呈爆发式增长：四类违法问题突出

https://mp.weixin.qq.com/s/29uKZDd1U9o-neR1N74xSg

谢谢！